An Energy Efficient ATM System Using AES Processor

Ali Nawaz*[1], Fakir Sharif Hossain[2], Khan Md. Grihan[3]

[1]Department of Electrical and Electronic Engineering

International Islamic University Chittagong, Dhaka, Bangladesh

*[1]just.piash@gmail.com;[2]sharifo16@yahoo.com;[3]grihankhan@yahoo.com

Abstract

This paper presents a highly secured ATM banking system using an optimized Advanced Encryption Standard (AES) algorithm. Two levels of security are provided in this proposed design. Firstly we consider the security level at the client side by providing biometric authentication scheme along with a password of 4-digit long. Biometric authentication is achieved by considering the fingerprint image of the client. Secondly we ensure a secured communication link between the client machines to the bank server using an optimize energy efficient AES processor. The fingerprint image is the data for encryption process and 4-digit long password is the symmetric key for the encryption process. To get a low power consuming ATM machine, an optimized AES algorithm is proposed in this paper. In this system biometric and cryptography techniques are used together for person authentication to improve the security level . The proposed design is secured against all kinds of attacks. The design of the processor is simulated on the FPGA platform. Simulation results ensure its proper functionality. The speed performance of the processor is also analysed and compared with that of other researchers in ASIC technology which also proves its superiority over them.

Keywords

Biometric; ATM; Fingerprint; Cryptography; AES Processor; Low Power

Introduction

Nowadays security becomes a great issue in every part of life. Passing of information faces massive problems due to various types of attacks into the communication link. A lot of researchers are working in the field of communication security. Many security algorithms are available to protect information from being hacked.

The biometric authentication process adds a new dimension of security for any person sensitive to authentication. This paper presents a secured and an energy efficient ATM banking system that is highly secured system compared with the existing ATM banking system. AT present most of the ATM systems use triple-data Encryption Standard (DES). But the triple-DES has some drawbacks. It is vulnerable to differential attacks and also slow in performance. This paper presents security in two ways. This design considers the fingerprint image for the client side security and also considers the AES algorithm for the secured communication in between the client and server. For these perspectives the Advanced Encryption Standard was accepted as a FIPS standard in November 2001. After that AES became the most popular encryption standard all over the world. A lot of researchers are working to improve the speed of AES as well as the other aspects like area, latency, power etc. To make the AES faster and securer some researchers introduced hardware realizations and s-box optimizations. Today most of the researchers involving the execution of the Advanced Encryption Standard (AES) algorithm are fallen into three areas: ultra-high-speed encryption, very low power consumption, and algorithmic integrity.

Many research works have been done by different hardware realizations using ASIC and FPGA technology. Some References present the fastest FPGA realization of the AES algorithm. Fingerprint based authentication is more secure, reliable and standard than the password based authentication. Finger-scan biometric is based on the distinctive characteristics of the human fingerprint. Our existing ATM system is password based. The limitation of this system is that it fails to identify the person rather it only identify the card and password as well as the communication link is not secured. , which have access to be hacked. The proposed ATM system is able to overcome this type of limitations because proposed ATM system is fingerprint based. Here

fingerprint is used as password which is encrypted by algorithm. This encrypted process is called Cryptography, the technique, way, process and science of hiding data that plays an important role to ensure information security. The encrypted data is decrypted by using same algorithm and matched with the stored data. If the data matched, the access will be granted otherwise access will be denied.

Background

ATM is the abbreviation of "Automated Teller Machine". This machine allows the account holder to have transactions with their own accounts without allowing them to access the entire bank's database. The idea of self-service in retail banking was developed through independent and simultaneous efforts in Japan, Sweden, the United Kingdom and the United States. In the USA, Luther George Simjian has been credited with developing and building the first cash dispenser machine. The first cash dispensing device was used in Tokyo in 1966.

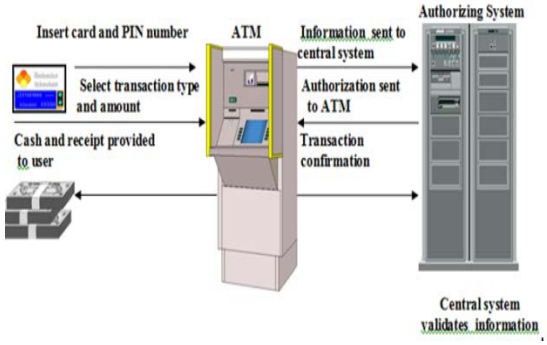

FIG. 1 A CONVENTIONAL ATM SYSTEM

ATM first came into use in December 1972 in the UK. IBM 2984 was designed for request of Lloyds Bank. ATM is typically connected directly to their hosts or ATM Controller via either ADSL or dial-up modem over a telephone line or directly via a leased line. For transaction security all communication traffic between ATM and transaction process is encrypted by cryptography. Nowadays, most of ATM uses a Microsoft OS primarily Windows XP Professional or Windows XP Embedded or Linux.

Fingerprint

Fingerprint is a characteristic which is unique for each person. Every fingerprint contain unique identifiable piece of information. The uniqueness in each fingerprint is due to the peculiar genetic code of DNA in each person. Ridges and valleys are the parts of fingerprint that provide friction for the skin. The direction and location of ridges make the identification. A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human. There are three types of fingerprint patterns.

AES Algorithm

The Rijndael algorithm referred to as the AES Algorithm, is a symmetric key block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Fig .1 shows that AES has four stages which are required for every round except that the last round excludes the mix column phase and the first round has only key addition.

The four stages of Rijndael algorithm (AES algorithm) are:

Substitute bytes: This function uses an S-box to perform a byte-by-byte substitution of the block. For encryption and decryption, this function is indicated by SubBytes () and InvSubBytes () respectively.

*Shiftrows:*This is a simple permutation. For encryption and decryption, this function is indicated by ShiftRows () and InvShiftRows () respectively.

Mix Columns: This is a substitution that makes use of arithmetic over GF (2^8), with the irreducible polynomial "$m(x) = x^8 + x^4 + x^3 + x + 1$". For encryption and decryption, this function is indicated by MixColumns () and InvMixColumns () respectively.

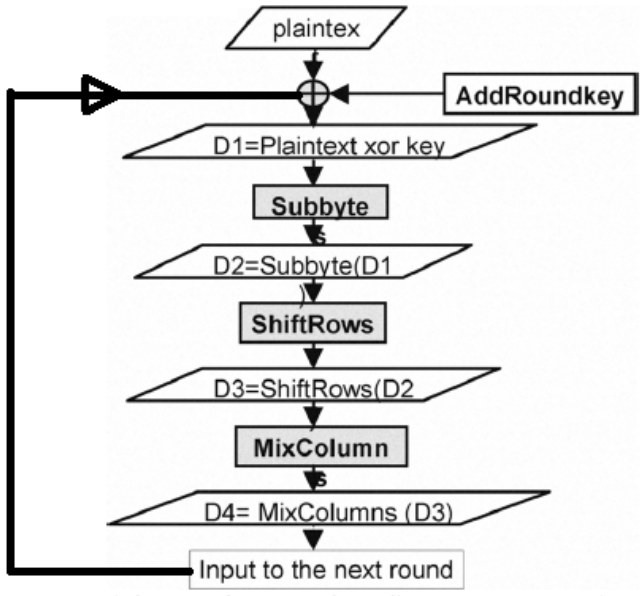

FIG. 2 AES ENCRYPTION AND DECRYPTIONS

Add round key: This function does a bitwise XOR operation of the current block with a portion of the expanded key. For both encryption and decryption this function is indicated by AddRoundKey (). For the AddRoundKey () stage, the inverse is achieved by XORing the same round key to the block, using the result: A ⊕A⊕ B = B.

Design Considerations

In this section, we present the design consideration of proposed ATM system to achieve highly secured and low power consumed ATM design. The two basic parts of this design are the biometric and cryptography.

Fingerprint Design

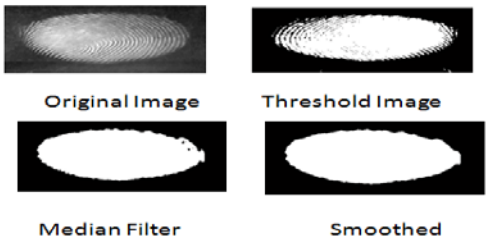

FIG. 3 FINGERPRINT IMAGE AND ITS PROCESSING STEPS

Original Image: The image is captured using image sensor.

Threshold Image: Only picking the pixel greater than the threshold pixel value.

Median Filter: The Median Filter block replaces the central value of an M-by-N neighbourhood with its median value.

Smoothed: Picking only the largest block.

Projected Area: Giving boundary line of the smoothed image on original image.

Rotate & Cropped: Aliening the major axis parallel with X axis taking only the fingertip part of the image.

Edge of Ridge: Binary value of the fingertip part using canny edge method.

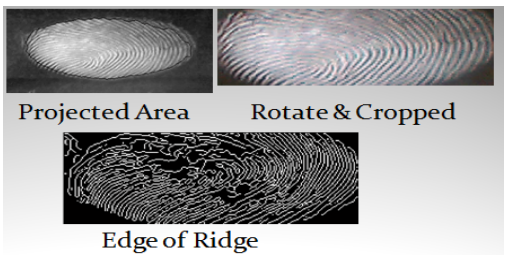

FIG. 4 FINGERPRINT IMAGE PROCESSING STEPS

Low Power Design of AES Processor

To get low power AES processor for minimizing the overall power consumption of the ATM system, we propose the S-box implementation in Galios Field $(2^4)^2$ instead of GF (2^8). S-box is the most costly transformation in AES, on the aspect of both time and area. Rijme one of the references suggested an alternative approach to calculate multiplicative inverses in S-Box. Since then, the relevant research has proved that the composite field $GF(2^4)^2$ based arithmetic provides the least gate count and the shortest critical path for calculating multiplicative inverse of a byte, which is the key step in S-Box. This conversion involves an isomorphic map function before and after inversion in each round. In our design we take 128-bit key for the AES processor, so it needs ten map functions for each block (128-bit) from finite field to composite field and ten inverse map functions for encryption. And the key generator, also has S-Boxes, is included, another ten mappings and ten inverse mappings are needed. Fig.5 shows the mapping of $GF(2^4)^2$.

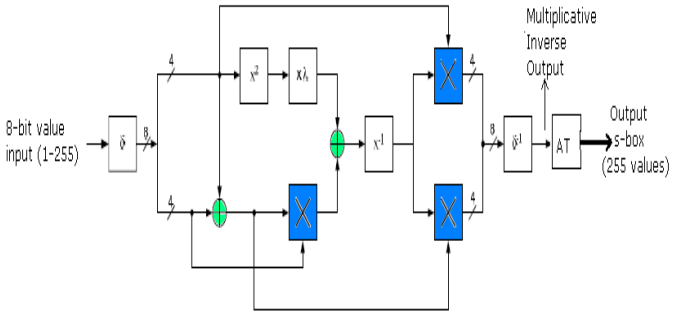

FIG.5 MULTIPLICATIVE INVERSION MAPPING IN$GF(2^4)^2$

To save the overhead caused by mapping, our design converts the whole AES algorithm from GF(2^8) to $GF(2^4)^2$, which needs only one forward mapping before the initial round and one backward mapping after the final round. Only one forward mapping is needed for the key schedule.

Proposed System and Performance

Proposed System

The proposed system consists of a fingerprint-capturing device, which captures image of the client. Captured image is fed to the image-processing device within the ATM machine. The processed image is converted to 1024 bit of binary data which is the input data of the low power consumed high

speedy AES processor. The AES processor encrypts the data with the help of 4 digit decimal key that is provided by the user as password. The data is encrypted and passed to the bank server through a communication link. At the bank side the received cipher message is decrypted with the same key. The original image is reproduced at this step. Then the decrypted image of fingerprint is matched with the previously stored image of the authentic customer for the specific request of the client. If the request is valid then an acknowledgement message is passed to the ATM machine through the same communication link. If the acknowledgement is "Yes" then client can withdraw money from the ATM machine. If acknowledgement is "No" an error message is shown on the screen of the ATM machine. In this paper we design an acknowledgement device which switches on a green light if the acknowledgement is "Yes" otherwise it turns to a red light. Fig.6 shows the proposed ATM system.

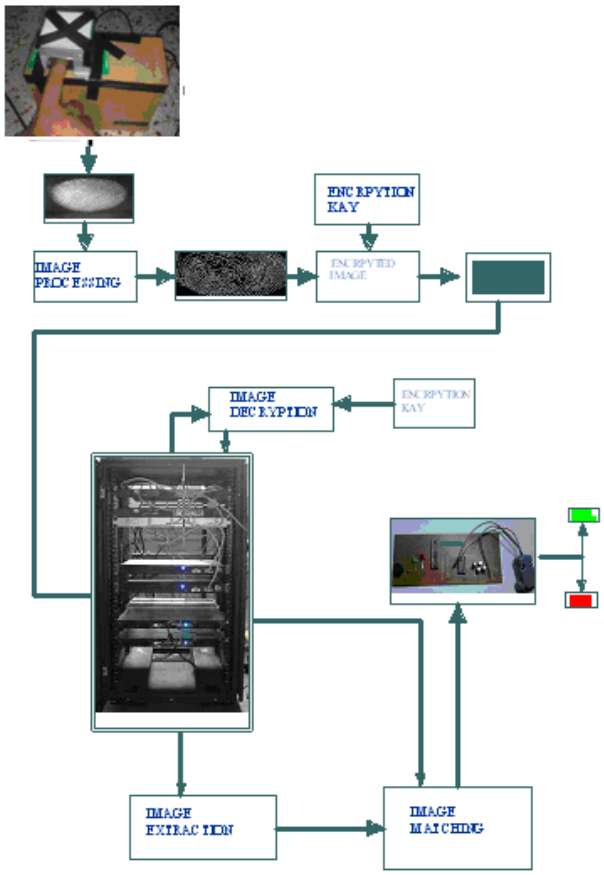

FIG. 6 PROPOSED ATM SYSTEM

Hardware Implementation

This proposed system has two hardwires; firstly an image acquisition device. Fig. 7 illustrates the image acquisition device. It consists of a prism and webcam which are mounted on a wooden box. The main function of this device is capturing the fingerprint and sending it to the processor for processing.

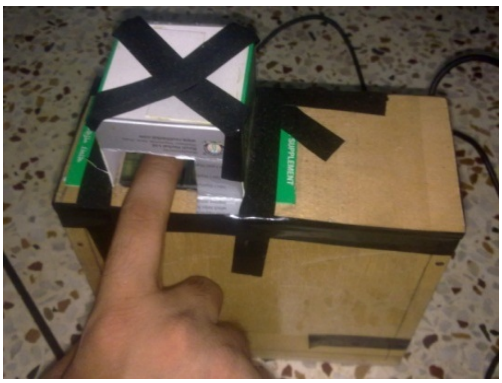

FIG. 7 IMAGE ACQUISITION DEVICE

The acknowledgement device provides the results if the matching processes are accurate. Fig. 8 shows the microcontroller based acknowledgement device. The acknowledgment device contains a red LED and a green LED. The communication link delivers the data to the main server. The processor sends the matching result serially into the microcontroller driven acknowledgment device through the serial port. If the stored image and the decrypted image match, the acknowledgment device turns on the green LED and the user can access to his or her account. On the other hand if the acknowledgement is negative, it turns on red LED. Consequently the access will be denied.

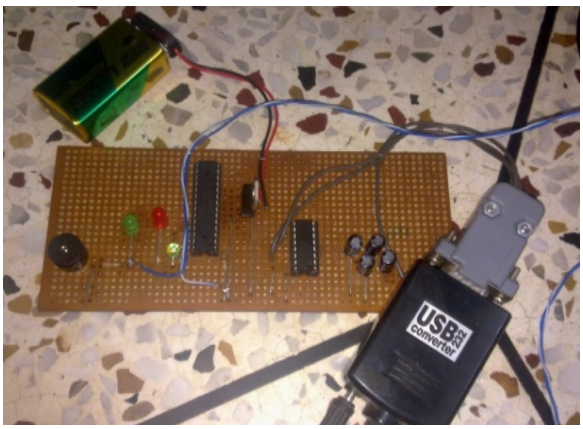

FIG. 8 ACKNOWLEDGEMENT DEVICE

Performance

The proposed system is one of the fastest and secured among the world's existing ATM systems. There are two reasons; firstly acquisition device captures image accurately. The error of the device is negligible. Secondly using AES with low power consumed high speedy AES processor makes the

system more secured and energy efficient, which makes the communication link secure.

Conclusion

Biometric authentication scheme for ATM banking system using energy efficient AES processor is presented in this paper. A number of novel design considerations have been adapted in designing the ATM system. It is capable of safeguarding against all known attacks. The whole system is simulated in quartus-II software. The simulation result shows the proper functionality of the system. The hardware implementation also carried out by implementing the LED based signaling. The encrypted message is sent to the server and compared with the stored fingerprint image. If the decrypted image and stored image are matched together, then a green led is on, otherwise a red led on. The hardware also shows the proper functionality of the system.

REFERENCES

Ali, L., Roy, N. and Faisal, F. F. " Design of a High Speed and Low Latency Crypto-processor ASIC" Semiconductor Electronics, 2008. ICSE 2008.

Brian, Milligan (25 June 2007), "The man who invented the cash machine", BBC News, Retrieved 26 April 2010.

Chandrakasan, A., Bowhill, W., "Design of High – Performance Microprocessor Circuits", (IEEE Press) 2001.

Dyken, J. V. and Delgado-Frias, J. G. "FPGA schemes for minimizing the power-throughput trade-off in executing the Advanced Encryption Standard algorithm" School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164-2752, USA, Available online 16 December 2009.

Federal Information Processing Standards Publication (FIPS PUB) 197, National Institute of Standards and Technology (NIST). (2001, November). Advanced encryption standard (AES). Available: http://csrc.nist.gov/publication/drafts/dfips-AES.pdf.

Gaj, K. and Chodowiec, P. "Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays", CT-RSA 2001, LNCS 2020, pp. 84-99, 2001.

Hodjat, A., Verbauwhede, I., "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA", 12th IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2004), pages 308-309, IEEE Computer Society, 2005.

Jarvinen et al. "A fully pipelined memoryless 17.8 Gbps AES-128 encryptor", International Symposium on Field Programmable Gate Arrays, pp. 207-215. 2003.

Joarvinen, K. "study on high-speed hardware implementation of cryptographic algorithm" Department of Signal processing and Acoustics, Helsinki University of technology, 10 Feb 2009.

Nachiketh, R., Potlapally, A. R." A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols," IEEE transaction on mobile computing, vol. 5, no. 2, February 2006.

Perrig, A., Wen, V., et at. "SPINS: security protocol for sensor networks," Wireless Network", 2002, 8(5), pp. 521-534.

Saggese et al. "An FPGA-Based Performance Analysis of the Unrolling, Tiling, and Pipelining of the AES Algorithm", FPL 2003, LNCS 2778, pp. 292-302, 2003.

Satoh et al. "A Compact Rijndeal HardWare Architecture with S-box Optimization" ASIACRYPT 2001, LNCS 2248, pp. 239-154, 2001.

Satoh, A., Morioka, S. and Takano, K. et al. "A compact Rijndael hardware architecture with S-Box optimization", In Proc.

Selvaraju, N. and Sekar, G. "A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm"International Journal of Computer Applications (0975 – 8887) Volume 3 – No.6, June 2010

Standaert et al. "Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs. " CHES 2003, LNCS 2779, pp. 334-350, 2003.

Ali Nawaz was born in Khulna, Bangladesh at 1990. He received his B. Sc. in Electrical and Electronic Engineering from International Islamic University Chittagong, Bangladesh in 2012.He also finish Cisco Certified Network Associate course in American International University Bangladesh 2012. Currently he is working as a Design & IT engineer in Electro Mech. Automation &Engineering Ltd. His areas of interest include Network Security, Cryptography, Automation, Renewable Energy, and Embedded system design.

Fakir S. Hossain was born in Dhaka, Bangladesh in 1984. He received his B. Sc. in Electrical and Electronic Engineering from Ahsanullah University of Science and Technology, Bangladesh in 2007. He also received his Post Graduate Diploma in Information Technology from University of Dhaka, Bangladesh in 2009. He received his M. Sc. in Information and Communication Technology from Bangladesh University of Engineering and Technology, Bangladesh in 2012. Currently he is working as a Lecturer in the Department of Electrical and Electronic Engineering, International Islamic University Chittagong (Dhaka Campus), Bangladesh. His areas of interest include Cryptography, Renewable Energy, Network Security, VLSI and Embedded system design.

Khan Md. Grihan received his B. Sc. in Electrical and Electronic Engineering from International Islamic University Chittagong, Bangladesh in 2011.Now he is doing his MBA in University of Dhaka, Bangladesh. Currently he is working as an Automation engineer in Electro Mech. Automation & Engineering Ltd. His areas of interest include FPGA, HMI, PLC, Microcontroller and Computer based Automation system development as well as in Image Processing and GUI designing.